UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/591,708	06/09/2000	Stuart J. Jacobs	00-8010	2685

25537 7590 02/12/2008

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
02/12/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

Office Action Summary	Application No.	Applicant(s)	
	09/591,708	JACOBS ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-12 and 14-22* is/are pending in the application.

4a) Of the above claim(s) *7,13, and 23* is/are ~~withdrawn from consideration.~~ Canceled.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-12 and 14-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-6, 8-12, and 8-22 remain pending.

Claims 7, 13, and 23 are cancelled.

Response to Arguments

2. Applicant's arguments, see Amendment After Non-Final Rejection, filed 11/15/2007, with respect to the rejection(s) of claim(s) 1-6, 8-12, and 14-22 under 35 U.S.C. 103(a) as being unpatentable over Minear, et al. (US 5,983,350), and further in view of Mason (US 5,668,998) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Minear and Gennaro.

Regarding argument on pg.13 (2nd paragraph) for claim 1, Minear discuses a working master copy...initialized at startup/initialization is not "based on the input" as claimed. The claimed input can broadly and reasonably interpret as an incoming packet/datagram/message or merely a request indication or entry where a device/user sending a request would constitute as receiving an input. The message or request may contain data (i.e. encrypted, hash, signed, etc.) that requires decryption or authentication (cryptographic related processing) to obtain the original content. For example, Minear discloses the proxy initiate an authentication protocol which can

include challenge/response authentication process and looks to see whether execution of an authentication and identification protocol is warranted or the message coming was encrypted (col.5, lines 37-45 and col.6, lines 14-20). Thus, obviously suggests an input requiring cryptographic related processing is received if challenge/response authentication process is initiated and that a determination whether encryption or authentication is warranted. In addition, Minear discloses when a dynamic entry is found, the current datagram's SRC address, which is required to ensure that the return datagram are properly encrypted (col.11, lines 30-34). Minear discussing the crypt-des decrypt function is for use by the IP input processing to decrypt a datagram (col.12, lines 5-13 and 41-47). The input or authentication protocol response is associated to a Security Association (SA) where the message is decrypted based on the algorithm and key associated with the particular SA (col.6, lines 10-12 and 32-36). Minear discloses IPSEC takes the standard Internet packet and converts it into a carrier packet. To use IPSEC, the SA is created for each destination IP address where this is the generated message based on the discussed input above (col.3, lines 8-36 and col.3, line 60-col.4, line 3). The claimed message representing a predefined message is the SA in the security association lookup or SADB because it contains algorithms, keys, etc. that corresponds to the received datagram (input requiring cryptographic related processing) that must be used to process the datagram correctly (col.4, lines 47-63). Therefore, Minear reads on the claimed receiving input requiring cryptographic related processing and the generated SA message is based on the input where the SA message representing one of a predefined set of messages.

Regarding argument on pg.14-15, Minear cannot read on "generating a message via the application program...". Minear discloses an application executing in application layer can communicate to an application executing by preparing a message (col.5, lines 50-53). Thus, by preparing a message can obviously suggest generating a message. Therefore, reads on generating a message via the application program. Minear discusses both input and output. Hence, by referencing certain SA information as output does not cover the entire understanding of what other information the SA contains. Minear discusses the ESP key to used for decryption of input datagrams and the AH key to be used for validation of input packets (col.4, lines 22 and 26). As discussed above, Minear discloses the crypt-des decrypt function is for use by the IP input processing to decrypt a datagram (col.12, lines 5-13 and 41-47) and the input or authentication protocol response is associated to the (SA) where the message is decrypted based on the algorithm and key associated with the particular SA (col.6, lines 10-12 and 32-36). Minear discloses IPSEC takes the standard Internet packet and converts it into a carrier packet. To use IPSEC, the SA is created for each destination IP address where this is the generated message based on the discussed input above (col.3, lines 8-36 and col.3, line 60-col.4, line 3). The claimed message representing a predefined message is the SA in the security association lookup or SADB because it contains algorithms, keys, etc. that corresponds to the received datagram (input requiring cryptographic related processing) that must be used to process the datagram correctly (col.4, lines 47-63). Thus, the message or datagram is obviously predefined since it is associated algorithm and key to the SA so that the message can be decrypted

accordingly to when it was encrypted. Minear suggests the claimed generating a message via an application program based on the input representing one of a predefined set of messages.

Regarding argument on pg.16-18 for claim 5, the arguments are addressed above because they are similar to the ones on pg.14-15.

Regarding argument on pg.19, that Minear does not suggest "...instructions which...transmitting...executed by the processor". Minear discloses the particular Security Parameter Index and a particular Destination Address uniquely identifies the SA (col.4, lines 40-42). The algorithm, keys, etc is determined to be used to process the datagram correctly where the information is obtained via a SA lookup and the lookup is being done to receive or transmit a datagram (col.4, lines 50-58 and 63-65). Hence, suggests instructions to perform transmitting based on the input...executed by the processor.

Gennaro is brought forth include the teaching of a well known art technology of PKI.

Regarding argument for claims 9, 14, and 22, have been addressed above and rejected with the same rationale as claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-4, 9-12, 14-18, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Minear, et al. (US 5,983,350), and further in view of Mason (US 5,668,998).

As per claim 1:

Minear teaches in a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions comprising:

executing an application program in a user space at the node; **(col.5, lines 50-58)**

receiving an input **(col.5, lines 37-45 and col.6, lines 13-27)** requiring cryptographic-related processing; **(col.11, lines 30-33 and col.12, lines 5-7 and 41-47)**

generating a message **(col.3, lines 8-36 and col.3, line 60-col.4, line 3)** via the application program based on the input **(col.5, lines 37-53)**, the message representing one of a predefined set of messages for processing by one of a plurality of cryptographic processing component in a kernel space located within the network node; **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

transmitting the message to one of a socket handler *[and a call handler]* in kernel **(col.5, lines 59-63)** space at the node to obtain a transmitted message; **(col.7, lines 43-54)**

forwarding the transmitted message to a request handler at the node **(col.12, lines 41-48)** which generates a function call to the cryptographic processing component appropriate for the transmitted message; **(col.5, lines 23-25 and col.11, line 54 – col.12, line 12)**

performing the cryptographic-related processing by the cryptographic processing component appropriate for the transmitted message. **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

Minear discloses the claimed socket handler to obtain a transmitted message in the form of a PF-SADB socket where it is much like a routing socket and is for processing to receive client requests (col.7, lines 27-32 and 43-45). Minear also discloses the claimed request handler that generates a function call to the cryptographic processing component as the required information is stored in a request structure that is bound to the IP datagram being processed where the request is of type crypto_request_t (col.11, lines 64-66). Minear further discusses one function, the cyl_enqueue_request is used to initiate either an encrypt or a decrypt action where this function is designed to be called by the cryptographic engine interface (col.12, lines 41-43). Minear discloses communications between workstations to an unprotected network or to another system (col.5, lines 34-58) where all network traffic must pass through one of the proxies within application layer before being transferred across network is allowed

and that a message arriving from the external network is examined at the IP layer (col.6, lines 35-37). Minear further discusses that when a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted (col.11, lines 30-37). Thus, suggests a function call to obtain a transmitted messages. Minear did not particularly discuss a handler (i.e. call handler).

Mason discloses an invention that presents an API which maps the DICOM standard services menu onto a framework of service interface objects which perform a selected DICOM services within or between PACS networks (col.1, line 66 – col.2, line 3). Mason explains that each service interface object is uniquely associated with a user handler and a provider handler wherein the association with a user/provider handler pair enable the pair to "handle" communications for the associated service interface object (col.2, lines 7-9). Mason further discusses the user handler enables an application to send a user-specified DICOM-encoded file message to a specified destination using the association control protocol. A provider handler receives the user-specified DICOM-encoded SEND message from an open association, stores the data set in a file, and reports to the requesting application (call back), upon completion of the requested service (col.13, lines 15-22). Hence, user/provider handler obviously suggests a call handler to obtain a transmitted message.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear with Mason to teach a call handler as a user/provider

handler pair because this enables the pair to handle communications for the associated message of the service request (Mason – col.2, lines 7-9 and col.13, lines 15-22).

As per claim 2: **See Minear on col.4, lines 1-28 and col.11, lines 46-53;** discusses the method of claim 1, wherein the cryptographic-related processing includes at least one of: verifying or generating a digital signature; encrypting data; decrypting data, retrieving a digital certificate or certificate revocation list; retrieving, verifying the hierarchy, and self-signed certificate processing within the node; or certificate age checking.

As per claim 3: **See Minear on col.6, line 66 – col.7, line 6 and 26-45;** discusses the method of claim 1, wherein transmitting includes: generating a user datagram (UDP) message containing an identifier associated with a predetermined cryptographic related functions and transmitting the UDP message via a UDP socket to the socket handler.

As per claim 4: **See Minear on col.11, line 54 – col.12, line 22;** discusses the method of claim 1 generating an output message via the application program wherein the output message requiring cryptographic-related processing, transmitting based on the required cryptographic-related processing, one of the predefined set of messages to the cryptographic processing component; performing the cryptographic-related processing, and outputting the processed message.

As per claim 9:

Minear discloses a cryptographic module, comprising:

a memory configured to store a plurality of cryptographic processing programs in user space on a computer-readable medium, each program being invoked via one of a plurality of predefined messages; and **(col.5, lines 50-58)**

a processor configured to:

receive an input **(col.5, lines 37-45 and col.6, lines 13-27)** requiring cryptographic-related processing, **(col.11, lines 30-33 and col.12, lines 5-7 and 41-47)**

generates one of predefined messages based on the input **(col.3, lines 8-36 and col.3, line 60-col.4, line 3)**, transmit the message to the first one of the cryptographic processing programs, and to perform, in kernel space, the cryptographic-related processing; **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

wherein the module receives, generates, transmits and performs through infrastructure comprising:

user space components including a user application program, a control daemon, a certificate database, a operations daemon and a remote server daemon; and **(col.5, lines 60-63 and col.6, lines 7-12 and 32-48)**

kernel space components including socket handler **(col.7, lines 43-54)**, *[a call handler]* and a request handler; and **(col.5, lines 23-25 and col.11, line 54 – col.12, line 12)**

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components **(col.12, lines 41-48)** communicate with other of the kernel space components; and **(col.5, lines 34-55 and col.6, lines 7-12 and 32-40)**

wherein other certain of the user space components communication with other certain of the kernel space components. **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

Minear discloses the claimed socket handler to obtain a transmitted message in the form of a PF-SADB socket where it is much like a routing socket and is for processing to receive client requests (col.7, lines 27-32 and 43-45). Minear also discloses the claimed request handler that generates a function call to the cryptographic processing component as the required information is stored in a request structure that is bound to the IP datagram being processed where the request is of type crypto_request_t (col.11, lines 64-66). Minear further discusses one function, the cyl_enqueue_request is used to initiate either an encrypt or a decrypt action where this function is designed to be called by the cryptographic engine interface (col.12, lines 41-43). Minear discloses communications between workstations to an unprotected network or to another system (col.5, lines 34-58) where all network traffic must pass through one of the proxies within application layer before being transferred across network is allowed and that a message arriving from the external network is examined at the IP layer (col.6, lines 35-37). Minear further discusses that when a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted (col.11, lines 30-37). Thus, suggests a function call to obtain a transmitted messages. Minear did not particularly discuss a handler (i.e. call handler).

Mason discloses an invention that presents an API which maps the DICOM standard services menu onto a framework of service interface objects which perform a

selected DICOM services within or between PACS networks (col.1, line 66 – col.2, line 3). Mason explains that each service interface object is uniquely associated with a user handler and a provider handler wherein the association with a user/provider handler pair enable the pair to "handle" communications for the associated service interface object (col.2, lines 7-9). Mason further discusses the user handler enables an application to send a user-specified DICOM-encoded file message to a specified destination using the association control protocol. A provider handler receives the user-specified DICOM-encoded SEND message from an open association, stores the data set in a file, and reports to the requesting application (call back), upon completion of the requested service (col.13, lines 15-22). Hence, user/provider handler obviously suggests a call handler to obtain a transmitted message.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear with Mason to teach a call handler as a user/provider handler pair because this enables the pair to handle communications for the associated message of the service request (Mason – col.2, lines 7-9 and col.13, lines 15-22).

As per claim 10: See Minear on col.4, lines 1-28 and col.11, lines 46-53; discusses the method of claim 9, wherein the cryptographic-related processing includes at least one of: verifying or generating a digital signature; encrypting data; decrypting data, retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; or certificate age checking.

As per claim 11: See Minear on col.5, lines 34-55 and Mason on col.2, lines 7-9; discusses the method of claim 9, wherein when transmitting the message, the processor is further configured to: transmit a function call to the first cryptographic processing program.

As per claim 12: See Minear on col.12, lines 1-16; discusses the method of claim 9, wherein the processor is further configured to: transmit the result of the cryptographic-related processing to an application program.

As per claim 14:

Minear discusses a method of performing cryptographic-related functions in a node coupled to other nodes in a network, the node includes an application program executed in user space for handling communications with the other nodes the method comprising:

receiving in said node an input **(col.5, lines 37-45 and col.6, lines 13-27)** requiring cryptographic-related processing; **(col.11, lines 30-33 and col.12, lines 5-7 and 41-47)**

generating in said node a predefined message based on the input **(col.3, lines 8-36 and col.3, line 60-col.4, line 3)**, the message one of a plurality of predefined message usable by of the cryptographic processing programs executed by one of a plurality of cryptographic processing component in a kernel space, each one of said messages being associated with a respective one of said cryptographic-related functions;

transmitting in said node a predefined message to a socket handler in kernel space or a call handler in kernel space to obtain a transmitted message; **(col.7, lines 43-54)**

forwarding the transmitted message to a request handler within the node **(col.12, lines 41-48)** which generates a function call to the cryptographic processing component appropriate for the transmitted message; **(col.5, lines 23-25 and col.11, line 54 – col.12, line 12)**

performing in said node, via cryptographic processing program the required cryptographic-related operation. **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

Minear discloses the claimed socket handler to obtain a transmitted message in the form of a PF-SADB socket where it is much like a routing socket and is for processing to receive client requests (col.7, lines 27-32 and 43-45). Minear also discloses the claimed request handler that generates a function call to the cryptographic processing component as the required information is stored in a request structure that is bound to the IP datagram being processed where the request is of type crypto_request_t (col.11, lines 64-66). Minear further discusses one function, the cyl_enqueue_request is used to initiate either an encrypt or a decrypt action where this function is designed to be called by the cryptographic engine interface (col.12, lines 41-43). Minear discloses communications between workstations to an unprotected network or to another system (col.5, lines 34-58) where all network traffic must pass through one of the proxies within application layer before being transferred across network is allowed and that a message arriving from the external network is examined at the IP layer (col.6,

lines 35-37). Minear further discusses that when a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted (col.11, lines 30-37). Thus, suggests a function call to obtain a transmitted messages. Minear did not particularly discuss a handler (i.e. call handler).

Mason discloses an invention that presents an API which maps the DICOM standard services menu onto a framework of service interface objects which perform a selected DICOM services within or between PACS networks (col.1, line 66 – col.2, line 3). Mason explains that each service interface object is uniquely associated with a user handler and a provider handler wherein the association with a user/provider handler pair enable the pair to "handle" communications for the associated service interface object (col.2, lines 7-9). Mason further discusses the user handler enables an application to send a user-specified DICOM-encoded file message to a specified destination using the association control protocol. A provider handler receives the user-specified DICOM-encoded SEND message from an open association, stores the data set in a file, and reports to the requesting application (call back), upon completion of the requested service (col.13, lines 15-22). Hence, user/provider handler obviously suggests a call handler to obtain a transmitted message.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear with Mason to teach a call handler as a user/provider handler pair because this enables the pair to handle communications for the associated message of the service request (Mason – col.2, lines 7-9 and col.13, lines 15-22).

As per claim 15: **See Minear on col.12, lines 1-16;** discusses the method of claim 14, returning the result of the performing to the application program.

As per claim 16: **See Minear on col.4, lines 1-28 and col.11, lines 46-53;** discusses the method of claim 14, a request for digital signature generation, a request for digital signature verification, a request for data encryption, a request for data decryption, a request for retrieval of digital certificate, a request verification of a certificate's hierarchy, a request for self-signed certificate processing, a request for certificate age checking.

As per claim 17: **See Minear on col.11, line 52 and col.12, line 18;** discusses the method of claim 16, wherein the request for digital signature generation includes a request for at least one of the RSA signature, secret key MD5 signature generation, elliptic curve signature generation or digital signature standard signature generation.

As per claim 18: **See Minear on col.4, line 8 and col.11, line 52 and col.12, line 18;** discusses the method of claim 16, wherein the request for digital signature verification includes a request for at least one of the RSA signature verification, secret key MD5 signature verification, elliptic curve signature verification or digital signature standard signature verification.

As per claim 21: **See Minear on col.10, lines 35-60;** discusses the method of claim 14, wherein the performing includes accessing a remote server via the network to retrieve cryptographic related information.

As per claim 22:

Minear discloses a computer-readable medium that stores instructions executable in user space by at least one processor in kernel space to perform a method for providing cryptographic-related functions, the method comprising:

receiving in at least one processor **(col.5, lines 37-45 and col.6, lines 13-27)** a first function call from a predefined list a first function call from a predefined list of function calls representing available cryptographic-related functions executable by the at least one processor; **(col.11, lines 30-33 and col.12, lines 5-7 and 41-47)**

generating in at least one processor in the environment a request message based on the first function call **(col.5, lines 23-25 and col.11, line 54 – col.12, line 12)**, a for cryptographic processing to further transmit the request message representing a request for processing by a cryptographic processing module executed by the at least one processor; **(col.3, lines 8-36 and col.3, line 60-col.4, line 3)**

transmitting in at least one processor the request message to the cryptographic processing module; and **(col.12, lines 41-47)**

performing in at least one processor the cryptographic-related function;

wherein the receiving, generating, transmitting and performing through infrastructure comprising:

user space components including a user application program, a control daemon, a certificate database, a operations daemon and a remote server daemon; and **(col.5, lines 60-63 and col.6, lines 7-12 and 32-48)**

kernel space components including socket handler, *[a call handler]* and a request handler; **(col.7, lines 43-54)**

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components **(col.12, lines 41-48)** communicate with other of the kernel space components; and **(col.5, lines 34-55 and col.6, lines 7-12 and 32-40)**

wherein other certain of the user space components communication with other certain of the kernel space components. **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

Minear discloses the claimed socket handler to obtain a transmitted message in the form of a PF-SADB socket where it is much like a routing socket and is for processing to receive client requests (col.7, lines 27-32 and 43-45). Minear also discloses the claimed request handler that generates a function call to the cryptographic processing component as the required information is stored in a request structure that is bound to the IP datagram being processed where the request is of type crypto_request_t (col.11, lines 64-66). Minear further discusses one function, the cyl_enqueue_request is used to initiate either an encrypt or a decrypt action where this function is designed to be called by the cryptographic engine interface (col.12, lines 41-43). Minear discloses communications between workstations to an unprotected network or to another system (col.5, lines 34-58) where all network traffic must pass through one of the proxies within application layer before being transferred across network is allowed and that a message arriving from the external network is examined at the IP layer (col.6, lines 35-37). Minear further discusses that when a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return

datagrams are properly encrypted (col.11, lines 30-37). Thus, suggests a function call to obtain a transmitted messages. Minear did not particularly discuss a handler (i.e. call handler).

Mason discloses an invention that presents an API which maps the DICOM standard services menu onto a framework of service interface objects which perform a selected DICOM services within or between PACS networks (col.1, line 66 – col.2, line 3). Mason explains that each service interface object is uniquely associated with a user handler and a provider handler wherein the association with a user/provider handler pair enable the pair to "handle" communications for the associated service interface object (col.2, lines 7-9). Mason further discusses the user handler enables an application to send a user-specified DICOM-encoded file message to a specified destination using the association control protocol. A provider handler receives the user-specified DICOM-encoded SEND message from an open association, stores the data set in a file, and reports to the requesting application (call back), upon completion of the requested service (col.13, lines 15-22). Hence, user/provider handler obviously suggests a call handler to obtain a transmitted message.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear with Mason to teach a call handler as a user/provider handler pair because this enables the pair to handle communications for the associated message of the service request (Mason – col.2, lines 7-9 and col.13, lines 15-22).

4. Claims 5-6, 8, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Minear, et al. (US 5,983,350) and Mason (US 5,668,998), and further in view of Gennaro (US 5,937,066).

As per claim 5:

Minear teaches a computer readable medium having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined messages, said instructions including sequences of instructions which, when executed by a processor in a user space, cause said processor to perform a method comprising:

receiving an input **(col.5, lines 37-45 and col.6, lines 13-27)** representing one of predefined messages; **(col.11, lines 30-33 and col.12, lines 5-7 and 41-47)**

transmitting, based on the input, a function call representing a request for cryptographic related processing to a cryptographic processing module executed by the process; and **(col.5, lines 23-25 and col.11, line 54 – col.12, line 12)**

performing the cryptographic-related processing by the cryptographic processing in a kernel space; **(col.6, lines 8-27 and col.11, lines 30-33)**

wherein at least the receiving the transmitting and the performing are implemented by *[public key authentication infrastructure (PKAI)]* comprising: **(col.3, line 57 – col.4, line 28)**

user space components including a user application program **(col.5, lines 50-58)**, a *[PKAI]* control daemon, a certificate database, a *[PKAI]* operations daemon and a *[PKAI]* remote server daemon; and **(col.5, lines 60-63 and col.6, lines 7-12 and 32-48)**

kernel space components including *[PKAI]* socket handler, *[a PKAI call handler]* and a *[PKAI]* request handler; and **(col.7, lines 43-54 and col.12, lines 41-48)**

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components communicate with other of the kernel space components; and **(col.5, lines 34-55 and col.6, lines 7-12 and 32--40)**

wherein other certain of the user space components communication with other certain of the kernel space components. **(col.6, lines 3-8 and 33-40 and col.7, lines 23-40)**

Minear discloses the claimed socket handler to obtain a transmitted message in the form of a PF-SADB socket where it is much like a routing socket and is for processing to receive client requests (col.7, lines 27-32 and 43-45). Minear also discloses the claimed request handler that generates a function call to the cryptographic processing component as the required information is stored in a request structure that is bound to the IP datagram being processed where the request is of type crypto_request_t (col.11, lines 64-66). Minear further discusses one function, the cyl_enqueue_request is used to initiate either an encrypt or a decrypt action where this function is designed to be called by the cryptographic engine interface (col.12, lines 41-43). Minear discloses communications between workstations to an unprotected network or to another system (col.5, lines 34-58) where all network traffic must pass through one of the proxies within application layer before being transferred across network is allowed and that a message arriving from the external network is examined at the IP layer (col.6,

lines 35-37). Minear further discusses that when a dynamic entry is found by a SPI search, the current datagram's SRC address, which is required to ensure that the return datagrams are properly encrypted (col.11, lines 30-37). Thus, suggests a function call to obtain a transmitted messages. However, Minear broadly suggests a handler for the function call (call handler) and PKAI.

Mason discloses an invention that presents an API which maps the DICOM standard services menu onto a framework of service interface objects which perform a selected DICOM services within or between PACS networks (col.1, line 66 – col.2, line 3). Mason explains that each service interface object is uniquely associated with a user handler and a provider handler wherein the association with a user/provider handler pair enable the pair to "handle" communications for the associated service interface object (col.2, lines 7-9). Mason further discusses the user handler enables an application to send a user-specified DICOM-encoded file message to a specified destination using the association control protocol. A provider handler receives the user-specified DICOM-encoded SEND message from an open association, stores the data set in a file, and reports to the requesting application (call back), upon completion of the requested service (col.13, lines 15-22). Hence, user/provider handler obviously suggests a call handler to obtain a transmitted message.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear with Mason to teach a call handler as a user/provider handler pair because this enables the pair to handle communications for the associated message of the service request (Mason – col.2, lines 7-9 and col.13, lines 15-22).

However, Minear and Mason combination did not include the cryptographic processing can be a public key infrastructure that includes authentication (PKAI). Gennaro discloses an invention that relates to a cryptographic key recovery system (col.1, lines 7-10) and that asymmetric encryption systems are generally more computationally intensive than symmetric encryption systems which are often used for highly sensitive data such as symmetric encryption keys (col.1, lines 39-45). Gennaro discusses the keyed shuffler function is an invertible function that transforms an n-bit input X into a shuffled n-bit output Y, that each bit in the output depends on each bit in the input (col.30, lines 58-65). The shuffler function calls for the function to handle an input of arbitrary length and produces a masked output (col.31, lines 1-11). Hence, suggests call handler that generates function call. Gennaro discloses a general public key infrastructure as the claimed PKAI where each key recovery agent has at least one public and private pair of keys that enables the use of public key cryptography to protect certain information until time to request decryption of this information (col.13, lines 65-col.14, line 9). Gennaro indicated the use of PKI are known in the art infrastructure that involves public/private signature (certification) keys for signing and public/private keys for encryption and distribution of keys. The means exists for the generation and distribution of these keys and that means exist for users to validate the public portion of these keys (col.25, lines 34-41).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear and Mason combination with Gennaro that authentication in a public key infrastructure (PKI) is a well known art for public/private

signature (certification) keys for signing and public/private keys for encryption and distribution of keys that enables the use of public key cryptography to protect certain information until time to request decryption of this information (Gennaro - col.13, lines 65-col.14, line 9 and col.25, lines 34-41).

As per claim 8: See Gennaro - col.1, lines 39-45 and col.13, lines 65-col.14, line 9 and col.25, lines 34-41; discussing the input represents a digitally signed network control message requiring verification.

As per claim 19: As rejected due to it dependency to claim 14 and further in view of Genarro; discusses the method of claim 16, wherein the request for data encryption includes a request for at least one of the RSA encryption or elliptic curve encryption.

However, Minear and Mason combination did not include the cryptographic processing can be the RSA encryption. Gennaro discloses an invention that relates to a cryptographic key recovery system (col.1, lines 7-10) and that asymmetric encryption systems are generally more computationally intensive than symmetric encryption systems. The asymmetric encryption system is often used for highly sensitive data such as encryption keys and that the best known an asymmetric encryption system is the RSA encryption system (col.1, lines 39-45).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear and Mason combination with Gennaro that the best known an asymmetric encryption system is the RSA encryption system where it is often used for highly sensitive data such as encryption keys and generally more

computationally intensive than symmetric encryption systems asymmetric (Gennaro - col.1, lines 39-45 and col.25, lines 34-41).

As per claim 20: As rejected due to it dependency to claim 14 and further in view of Genarro; discusses the method of claim 16, wherein the request for data decryption includes a request for at least one of the RSA decryption or elliptic curve decryption.

However, Minear and Mason combination did not include the cryptographic processing can be the RSA encryption. Gennaro discloses an invention that relates to a cryptographic key recovery system (col.1, lines 7-10) and that asymmetric encryption systems are generally more computationally intensive than symmetric encryption systems. The asymmetric encryption system is often used for highly sensitive data such as encryption keys and that the best known an asymmetric encryption system is the RSA encryption system (col.1, lines 39-45).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Minear and Mason combination with Gennaro that the best known an asymmetric encryption system is the RSA encryption system where it is often used for highly sensitive data such as encryption keys and generally more computationally intensive than symmetric encryption systems asymmetric (Gennaro - col.1, lines 39-45 and col.25, lines 34-41).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135